**P3 – Software & Network Security**

While physical security protects against most threats, there are still other avenues of attack. Particularly, any device connected to a network is at risk from any other device that can connect to the network – if the LAN the device is on is connected to the internet, then it faces potential threats from anywhere in the world.  
To counteract this, there is network and software security that protects against the threats that physical security doesn’t cover.

**Network Security**Physical security stops physical threats; network security stops threats from a network, which at the lowest level are all software-based threats. Therefore, good network security is the best and first defence against non-physical threats.  
Network threats can be internal or external, so it is important to protect against both types. External attacks come from outside the LAN – either a WAN or the internet. The vulnerable point for this type of threat is the access point for the WAN. On most networks this is the router. Home network users don’t really need to worry about this, as the chances of them being targeted by an attack are slim, and the security software on their PC is good enough.  
However, for larger networks, such as those used by companies or ones that run critical systems, they may invest in a high-end router that has its own firewall. A firewall analyses all data entering and leaving the network, and determines what is allowed to pass through. This prevents basic threats, such as somebody intercepting outgoing traffic and sending malicious code back.  
PC’s can have their own firewalls – most OS’s come with one, and anti-virus software will also often use a firewall. Used in conjunction with a router-based firewall. This makes it difficult for attackers to exploit weaknesses in networking protocols.  
Another form of security for networks is encryption. This makes it impossible for anybody intercepting communications to understand them. The most common form of encryption on the internet is probably HTTPS, the secure variant of the HTTP protocol. When data is sent with HTTPS, it is secure and cannot be used by anybody who intercepts it. This is why it’s used when logging into online services.  
Another form of encryption is WPA/WEP. This is used to encrypt all data sent between a device and a router over Wi-Fi. It also implements passwords on wireless networks, to ensure that only devices with the passcode can even connect to the network.

**Software Security**  
Software security prevents against software-based attacks, such as viruses or hacking. The most common method of software security is anti-virus, which protects against malicious software, or ‘malware’, such as viruses, worms, Trojans and other vulnerabilities on the PC. Modern anti-virus software can even analyse web pages and programs in real-time, so if they suddenly start behaving maliciously they can be stopped.